Oracle Access Manager Oracle Banking Treasury Management Release 14.4.0.0.0 [April] [2020]

FINANCIAL SERVICES

Table of Contents

| 1. | I | INTR | ODUCTION | |
|----|---|---------------------------------------|--|-----|
| 2. | BA | CKG | ROUND AND PREREQUISITES | 2-1 |
| | 2.1 | Pre | -REQUISITES | |
| | 2.1 | 1.1 | Software Requirements | |
| | 2.2 | BAC | CKGROUND OF SSO RELATED COMPONENTS | |
| | 2.2 | .1 | Oracle Access Manager (OAM) | |
| | 2.2 | .2 | LDAP Directory Server | |
| | 2.2 | .3 | WebGate/AccessGate | |
| | 2.2 | .4 | Identity Asserter | |
| | | | | |
| 3. | (| CONE | FIGURATION | |
| | (3.1 | | TGURATION | |
| | | Pre | | |
| | 3.1 | Pre Cha | -Requisites | |
| | 3.1 3.2 | Pre Cha Con | -REQUISITES | |
| | 3.1 3.2 3.3 | Pre Cha Con Firs | -REQUISITES INGE THE WEB.XML FILE IFIGURING SSO IN OAM CONSOLE | |
| | 3.1 3.2 3.3 3.4 | Pre ChA Con Firs | -REQUISITES INGE THE WEB.XML FILE IFIGURING SSO IN OAM CONSOLE ST LAUNCH OF ORACLE BANKING TREASURY MANAGEMENT AFTER INSTALLATION | |
| | 3.1 3.2 3.3 3.4 <i>3.4</i> | PRE CHA CON FIRS .1 .2 | -REQUISITES INGE THE WEB.XML FILE IFIGURING SSO IN OAM CONSOLE ST LAUNCH OF ORACLE BANKING TREASURY MANAGEMENT AFTER INSTALLATION SSO Parameters | |



1. Introduction

For the purpose of single sign-on ORACLE BANKING TREASURY MANAGEMENT is qualified with Oracle Identity Management 12.2.1.4.0 (Fusion Middleware 12c) – specifically using the Access Manager component of Oracle Identity Management. This feature is available in the releases OBTR_14.4.0.0.0 and onwards of ORACLE BANKING TREASURY MANAGEMENT.

This document is expected to provide an understanding as to how single sign-on can be enabled for a ORACLE BANKING TREASURY MANAGEMENT deployment using Oracle Fusion Middleware 12c.

In addition to providing a background to the various components of the deployment, this document also, talks about Configuration in ORACLE BANKING TREASURY MANAGEMENT and Oracle Access Manager to enable single sign-on using Oracle Internet Directory as a LDAP server.



2. Background and Prerequisites

2.1 <u>Pre-Requisites</u>

The following are the pre-requisites for Oracle Access Manager (OAM) and LDAP Directory Server.

2.1.1 Software Requirements

- 1. Oracle Access Manager OAM (12.2.1.4.0)
 - Access Server
 - Webtier Utilities 12.2.1.4.0
 - Web Gate 12.2.1.4.0
 - Http Server
- 2. LDAP Directory Server

Please make sure that the LDAP which is been used for ORACLE BANKING TREASURY MANAGEMENT Single Signon deployment is certified to work with OAM.

List of few LDAP Directory servers supported as per OAM document (note – this is an indicative list. The conclusive list can be obtained from the Oracle Access Manager documentation):

- Oracle Internet Directory
- Active Directory
- ADAM
- ADSI
- Data Anywhere (Oracle Virtual Directory)
- IBM Directory Server
- NDS
- Sun Directory Server
- 3. Web Logic 12.2.1.4.0

For the purpose of achieving single sign on for OBTR in FMW 12c, it is necessary for the weblogic instance to have an explicit Oracle HTTP server (OHS).



2.2 Background of SSO related components

2.2.1 Oracle Access Manager (OAM)

Oracle Access Manager consists of the Access System, and the Identity System. The Access System secures applications by providing centralized authentication, authorization and auditing to enable single sign-on and secure access control across enterprise resources. The Identity System manages information about individuals, groups and organizations. It enables delegated administration of users, as well as self-registration interfaces with approval workflows. These systems integrate seamlessly.

The backend repository for the Access Manager is an LDAP-based directory service that can be a combination of a multiple directory servers, which is leveraged for two main purposes:

- As the store for policy, configuration and workflow related data, which is used and managed by the Access and Identity Systems
- As the identity store, containing the user, group and organization data that is managed through the Identity System and is used by the Access System to evaluate access policies.

2.2.2 LDAP Directory Server

To integrate ORACLE BANKING TREASURY MANAGEMENT with OAM to achieve Single Sign-on feature, ORACLE BANKING TREASURY MANAGEMENT's password policy management, like password syntax and password7 expiry parameters can no longer be handled by ORACLE BANKING TREASURY MANAGEMENT. Instead, the password policy management can be delegated to the Directory Server. All password policy enforcements would be on the LDAP user id's password and NOT ORACLE BANKING TREASURY MANAGEMENT application users' passwords.

2.2.3 WebGate/AccessGate

A WebGate is a Web server plug-in that is shipped out-of-the-box with Oracle Access Manager. The WebGate intercepts HTTP requests from users for Web resources and forwards it to the Access Server for authentication and authorization.

Whether you need a WebGate or an AccessGate depends on your use of the Oracle Access Manager Authentication provider. For instance, the:



Identity Asserter for Single Sign-On: Requires a separate WebGate and configuration profile for each application to define perimeter authentication. Ensure that the Access Management Service is On.

Authenticator or Oracle Web Services Manager: Requires a separate AccessGate and configuration profile for each application. Ensure that the Access Management Service is On.

2.2.4 Identity Asserter

Identity Asserter uses Oracle Access Manager Authentication services and also validates alreadyauthenticated Oracle Access Manager Users through the ObSSOCookie and creates a WebLogicauthenticated session. It also provides single sign-on between WebGates and portals. We can get more details on Identity asserter <u>HERE</u>

This document containts the configuration of Oracle Interner Directory as LDAP server and its configuration in weblogic. This document will not discuss the configuring and setting up of OAM and LDAP directory server of other LDAP servers. This will be provided by the corresponding Software provider.



3. Configuration

3.1 Pre-Requisites

The steps provided below assume that ORACLE BANKING TREASURY MANAGEMENT has already been deployed and is working (without single sign-on)

The provided below steps assume that Oracle Access Manager and the LDAP server have been installed already and the requisite setup already done with respect to connecting the two along Weblogic's Identity Asserter.

3.2 Change the web.xml file

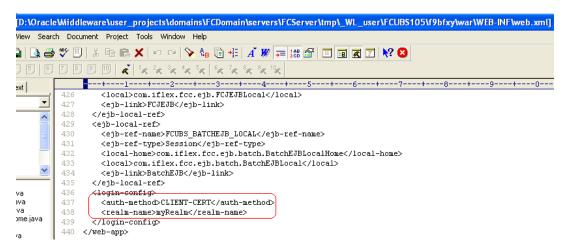
- 1. Locate the web.xml file in the application (OBTR) EAR file
- 2. Add the following lines under login-config.

<login-config>

<auth-method>CLIENT-CERT</auth-method>

<realm-name>myRealm</realm-name>

</login-config>



3. Save the file and redeploy and restart the application.



3.3 Configuring SSO in OAM Console

After installing OAM, Webtier Utilities and Webgate, extend the weblogic domain to create OAM server.

Follow the post installation scripts deployWebGate and EditHttpConf as provided in (<u>http://docs.oracle.com/cd/E17904_01/install.1111/e12002/webgate004.htm</u>

1. Identity Store Creation

To create new User Identity Store, Login to OAM Console and navigate to System Configuration>>Common configuration>>Data Sources>> User Identity Store.

2. Input below information in the User Identity Store.

Choose Store Type as Oracle Internet Directory.

Location:

LDAP server Host name and Port Number in <HOSTNAME>:PORT format

Bind DN:

User name to connect the LDAP Server

Password:

Password to connect the LDAP Server

User Name Attribute:

The attribute created in LDAP, which will be the User Name for the other application (here it will be treated as the OBTR Username)

User Search Base:

The container of the User Name in the LDAP server.

Group Search Base:

The container of the Group Name in the LDAP server.



| Common Configuration • Welcome • CUBSWebgate • OMM Agents • oam_server1 LDAP User Identity Stores · Create: User Identity Store · Store Name FOUBSIdentityStore · Store Type OD: Oracle Internet Directory · Store Type OD: Oracle Internet Directory · Create: User Identity · Create: User IdentityStore · Store Type OD: Oracle Internet Directory · ::: Create: User IdentityStore · ::: · ::: · Create: User IdentityStore · · · · · · · · · · · · · · · | Firefox Oracle Access Manager - Administrat | × 🗍 Error 404Not Found × + | \bigtriangledown | | × |
|---|---|--|--------------------|--------------|--------|
| Duck Contraction Specific training Spe | filchw-ap-21:7001/oamconsole/faces/pages/Po | icyManager,jspx?_adf.ctrl-state=kfr23iytk_4&_afrLoop=10370372111194 😭 🗢 🧭 🖓 🗸 oam agent 11g base url | ٩ | ↑ □ - | # |
| Duck Contraction Specific training Spe | DRACLE' Access Manager | | Accessibility | Help Sign | Out 🤇 |
| 2 Common Configuration Accors New / Configuration | | | | Signed in as | weblog |
| 2. Control Configuration Read: Week Read: Week <td< td=""><td>Policy Configuration System Configuration</td><td></td><td></td><td></td><td></td></td<> | Policy Configuration System Configuration | | | | |
| Actors - Verr Interface Interface - Verr Interface Actors - Verr Interface Actors - Verr Interface </td <td>X Common Configuration</td> <td>Welcome FCUB5Webgate OAM Agents oam_server1 LDAP User Identity Stores</td> <td></td> <td>×</td> <td></td> | X Common Configuration | Welcome FCUB5Webgate OAM Agents oam_server1 LDAP User Identity Stores | | × | |
| 2) Sources * Store Haste PLAGE > Access Hanger Settings * Store Type Disconde Internet Directory Image Part Part Part Part Part Part Part Part | | Create: User Identity Store | Test Connection | Apply | ? |
| V Buter Identity Stores > Water Identity Ident | ▼ Data Sources ▲ | * Store Name ECLIBSIdentityStore Description | | | = |
| > Declare Verwit > Access Manage Setting: > Consection Markers Setting: > Consection Markers Setting: > Consection Markers > Consection Markers > Consection Markers > Consection Markers > Setting: > Seting: > Setting: > Setting: > Setti | | | | | |
| ✓ Access Hanager Settings Costing Automation models In User Settings Costing Automation models In Cos | SubserIdentityStore1 | | | | |
| | ✓ Access Manager Settings | Enable SSL | | | |
| | Actions 🗸 View 👻 📑 🔁 🗶 🙀 | | | | |
| > Scotts Agents > Scotts Agents > Scotts Agents > Scotts Agents > Scotts Advented atom modele > Scotts Authentication Authenticatin Authentication Main Productin A | > S Access Manager Settings | * Location iffchw-ap-21:3061 * Bind DN cn=ordadmin | | | |
| ? ■ Users and Groups > ■ Users and Groups > ■ Users and Groups > ■ Groups Authentication modele > ■ Groups Cache State © Group Cache State Group Cache State (Mb) Operation @ Group Cache TTL (Seconde) @ Broups Authentication modele > ■ Group Cache State (Mb) @ Group Cache TTL (Seconde) @ Group Cache TTL (Seconde) @ Group Cache TTL (Seconde) @ Broups Authentication modele > ■ Security Token Service | | *Password ** | | | |
| all damentacion Medica all LAP bit | | Villsers and Groups | | | |
| > Bit DuPriePasswordAutHModule > Bit SD3 Authentiation module > Bit SD3 Authentiation module > Bit Coston Authentiation module Coston Authentiation module Bit Coston Authentiation module Coston Authentiation module Bit Coston Authentiation module Coston Authentiation module Coston Authentiation module Coston Authentiation module Coston Coston Bit Coston Authentiation module Coston Coston Bit Coston Authentiation module Wat Timeout (seconds) Bit Coston Authentiation module Security Token Service Security Token Service | | | | | |
| > Security Token Service | | * User Search Base cn=Users,dc=oracle,dc=com | | | |
| > if X39 Authentication module > if Costom Authentication module * Group Rame Attribute * Group Fater Base Group Cache Group Cache Size (Mb) 1 Connection Details Minimum Pool Size 10 if Maximum Pool Size 2 Security Token Service 2 Security Token Service | | User Filter Object Classes | | | |
| Comp Filer Classes Group Filer Classes Group Cache Group Cache TL (seconds) 0 0 Group Cache TL (seconds) 0 0 Maximum Pool Size 10 0 Maximum Pool Size 50 0 Maximum Pool Size 50 0 Maximum Pool Size 50 0 Retry Count 3 0 Maximum Pool Size 50 0 Ma | ▷ # X509 Authentication module | Group Name Attribute | | | |
| 2 Security Token Service | Custom Authentication module | | | | |
| Security Token Service | | Group Filter Classes | | | |
| Croup Cache TTL (Seconds) 0 € Connection Details Minimum Pool Size 10 € Maximum Pool Size 50 € Wat Timeout (seconds) 120 € Inactivity Timeout (seconds) 20 € Inactivity Timeout (seconds) 20 € Connection Details Results time limit (seconds) 0 € Referral Policy follow ▼ Inactivity Timeout (seconds) 20 € Connection Details Referral Policy follow ▼ | | Enable Group Cache | | | |
| Connection Details Minimum Pool Size 10 10 Maximum Pool Size 50 Results time limit (seconds) 0 Refral Policy follow Inactivity Timeout (seconds) 10 1 Inactivity Timeout (seconds) 1 | | Group Cache Size (Mb) 10000 🚔 | | | |
| Minimum Pool Size 10 mmm Maximum Pool Size 50 mmm Wait Timeout (seconds) 120 mmm Wait Timeout (seconds) 120 mmm Inactivity Timeout (seconds) 120 mmm Security Token Service 1 | | | | | |
| Maximum Pool Size 50 mm Wait Timeout (seconds) 120 mm Inactivity Timeout (seconds) 10 | | | | | |
| Wait Timeout (seconds) 120 🛱 Referral Policy follow Inactivity Timeout (seconds) 2 | | | | | |
| Security Token Service | | | | | |
| ≥ Security Token Service | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | > Security Token Service | | | | |
| | | | | | |
| | | | | _ | |

3. After input of the above information click on 'Apply' button. On successful creation, click test connection button to verify whether the LDAP connection is working fine.



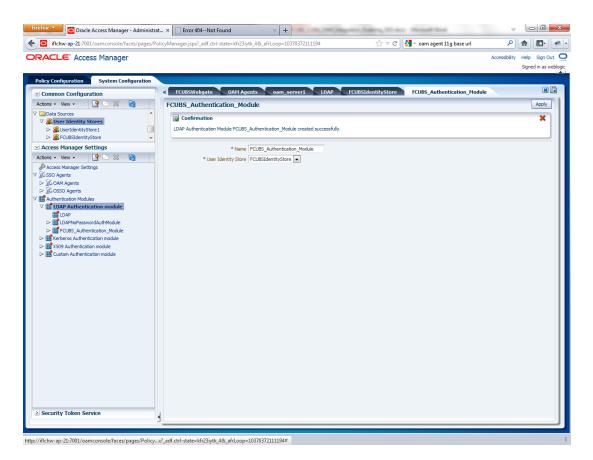
| Firefox Oracle Access Manager - Administra | t × C Error 404Not Found × + | ↓ □ □ × |
|---|---|---|
| (iflchw-ap-21:7001/oamconsole/faces/pages/P | olicyManager.jspx?_adf.ctrl-state=kfr23iytk_4&_afrLoop=10370372111194 👘 🛡 😋 🚼 🔹 oam age | ent 11g base url 🔎 🍙 💽 🕐 🔹 |
| ORACLE [®] Access Manager | | Accessibility Help Sign Out O |
| Policy Configuration System Configuration | | |
| Common Configuration | Welcome FCUBSWebgate OAM Agents oam_server1 LDAP FCUBSIdentityStore | |
| Actions 🕶 View 👻 📑 🗁 💥 🖓 | FCUBSIdentityStore | Test Connection Apply (?) |
| ∇ □ Data Sources ∇ ▲ User Identity Stores | Confirmation | Connection Status 🛛 💥 |
| Sor Identity Stores Sore a User Identity Store 1 Sore Store Sto | User Identity Store FCUBSIdentityStore created successfully. | Connection to the User Identity Store successful! |
| Section Sections | Store Name FCUBSIdentityStore Description | OK Cancel |
| Actions 🕶 View 👻 🔄 🔀 | * Store Type OID: Orade Internet Directory | |
| > Access Manager Settings | | ii. |
| | Enable SSL | |
| > 🖉 OSSO Agents | ✓ Location and Credentials | |
| ✓ ∰ Authentication Modules ✓ ∰ LDAP Authentication module | * Location ifichw-ap-21:3061 * Bind DN cn=orc | |
| | *Password ••••• | •• |
| DAPNoPasswordAuthModule | | |
| Kerberos Authentication module X509 Authentication module | Default and System Store Options Set as default store (Current Default Store UserIdentityStore 1) | |
| Custom Authentication module | Set as system store (Current System Store UserIdentityStore1) | |
| | ✓Users and Groups | |
| | * User Name Attribute uid | |
| | * User Search Base cn=Users,dc=orade,dc=com | |
| | User Filter Object Classes | |
| | Group Name Attribute | |
| | * Group Search Base cn=Groups,dc=oracle,dc=com | |
| | Group Filter Classes | |
| | Enable Group Cache | |
| | Group Cache Size (Mb) 10000 🖨 | |
| | Group Cache TTL (Seconds) | |
| | ✓ Connection Details | |
| | Minimum Pool Size 10 🗬 Results time limit (seconds | s) 0 🚔 |
| | Maximum Pool Size 50 🖶 Retry Coun | nt 3 🖨 |
| | Wait Timeout (seconds) 120 🚔 Referral Policy | y follow 💌 |
| Security Token Service | Inactivity Timeout (seconds) | |
| |) | |
| | | |

4. Creating Authentication Module

Navigate to System Configuration >> Access Manager Settings >> Authentication Modules >> LDAP Authentication Module.

Click 'New' Button to create new Authentication Module. Input the Name of the authentication module and choose the User Identity Store we created in step 1.





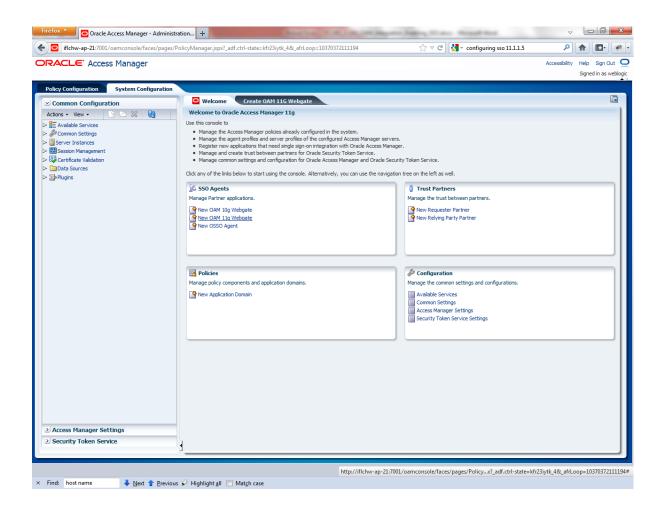
5. Creating OAM 12c Webgate

Navigate to System Configuration>>Access Manager Settings>>SSo Agents>>OAM Agents.

Click on 'Create 12c webgate' button

or Click on New OAM 12c Webgate link available in welcome page.





Enter any name for Webgate and Base URL (The host and port of the computer on which the Web server for the Webgate is installed) and click on apply.



| iflchw-ap-21:7001/oamconsole/faces/pages; | /PolicyManager.jspx?_adf.ctrl-state=kf | r23iytk_4&_afrLoop=10370372111194 | ☆ マ C 🖁 🗧 configuring sso 11.1.1.5 | ₽ 🟦 💽 🦸 |
|--|--|--|--|--|
| RACLE' Access Manager | | | | Accessibility Help Sign Out Signed in as webl |
| Policy Configuration System Configuration | | | | |
| Common Configuration | O Welcome Create 0/ | AM 11G Webgate | | X |
| Actions • View • 📑 🗁 💥 🔯 | Create OAM 11g Webga | te | | Apply |
| ► Available Services ► Common Settings ► Services ► Settings ► Settings ► Settings ► Settings ► Settings ► Data Sources ► Plugins | Base URL Access Client Password * Security | FCUBSWebgate http://fichw-ap-21:7001 .:i | User Defined Parameters Virtual host Auto Create Policies IP Validation | i. |
| > Access Manager Settings | | | | |
| | | | | |

Once the OAM 12c Webgate created, add filterOAMAuthnCookie=false parameter along with default parameters in User Defined Parameters.

Click 'Apply' button to save the changes.



| ifichw-ap-21:7001/oamconsole/faces/pages/Pol Access Manager | cyManager.jspx2_afrWindowMode=08i_afrLoop=2972696137720 | 38_adf.ctrl-state=1cm2g2efx, 🖓 ♥ C] [🔮 - filt | erOAMAuthnCookie parameter | Help Sign Out Signed in as weblogi |
|---|---|---|----------------------------|------------------------------------|
| Policy Configuration System Configuration Common Configuration Actions • View • • • • • • • • • • • • • • • • • • • | Welcome OAM Agents FCUBSWebgate CONFirmation OAM 11g Webgate FCUBSWebgate modified successfully. Application | ation Domain is FCUBSWebgate | | Apply |
| Access Manager Settings Actions View | Name FCUBSWebgate Access Clent Password | Logout Redirect URL Logout Target URL | no-cache | 10 |
| 2./ Security Token Service | Server List | Secondary Server List | umbe | · |

6. Post OAM Webgate 12c Creation Steps

Perform the following steps to copy the artifacts to the Webgate installation directory:

• On the Oracle Access Manager Console host, locate the updated OAM Agent ObAccessClient.xml configuration file (and any certificate artifacts). For example:

\$DOMAIN_HOME/output/\$Agent_Name/ObAccessClient.xml

• On the OAM Agent host, copy artifacts (to the following Webgate directory path). For example:

12cWebgate_instance_dir/webgate/config/ObAccessClient.xml

(for instance WebTier_Middleware_Home/Oracle_WT1/instances/instance1/config/ OHS/ohs1/webgate/config/ObAccessClient.xml)



7. Creating Authentication Scheme

To create Authentication Scheme navigate to Policy Configuration >> Authentication Schemes

Click on 'Create' button to create new Authentication Scheme.

| Name | : Any name to identify Authentication Scheme |
|------------------------|--|
| Challenge Method | : BASIC |
| Challenge Redirect URL | : /oam/server |

Authentication Module : Choose the authentication module created in step 2.

| Firefox Contracte Access Manager - Administra | st × 🖸 Integrating OAM Security Provider wi × 🕂 | |
|--|---|---|
| (iflchw-ap-21:7001/oamconsole/faces/pages/P | olicyManager.jspx?_adf.ctrl-state=kfr23iytk_4&_afrLoop=10370372111194 | ☆ マ C 👌 authentication schema oam 11g 🛛 👂 🏫 💽 🛛 🥐 🔹 |
| ORACLE' Access Manager | | Accessibility Help Sign Out 🧿 |
| - | | Signed in as weblogic |
| Policy Configuration System Configuration | | |
| All | O Welcome B FCUBS_Auth_Scheme | |
| Search | Authentication Schemes | Set As Default Apply |
| Image: Search Image: Started Components V Started Components V Image: Started Components Image: Started Components | Authentication Schemes Confirmation Authentication Scheme, FCUBS_Auth_Scheme, created successfully * Name FCUBS_Auth_Scheme Description * Authentication Level Defaul * Challenge Redirect URL / Joan/Server * Authentication Module FCUBS_Authentication_Module Challenge Parameters: | Set Ao Default Apply |
| Gerusion Apos Integration Gi TAM Suite | <u></u> | |



If it is a basic authentication scheme, we need to add the 'enforce-valid-basic-auth-credentials' tag to the config.xml file located under /user_projects/domains/<MyDomain>/config/. The tag must be inserted within the <security-configuration> tag as follows: [Just before the end of security configuration tag]

<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>

</security-configuration>

8. Creating Authentication Scheme

To create authentication policy, navigate to Policy Configuration >> Application Domains >> [Webgate agent name] >> Authentication Policies.

Click new button and input the below information

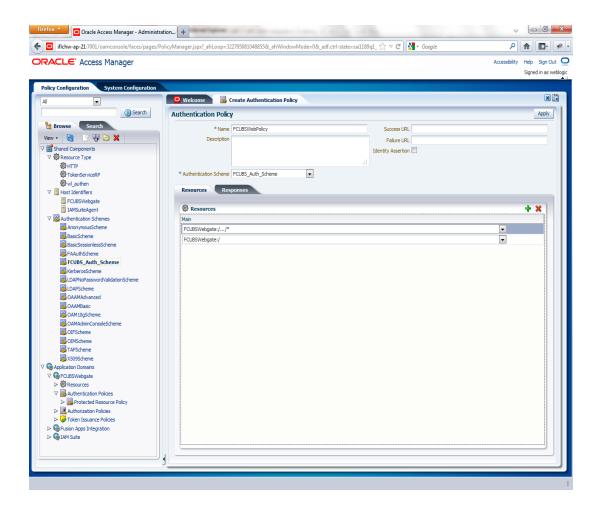
Name: Enter any name to identify the Authentication Policy (eg. OBTRWebPolicy)

Authentication Scheme: Choose the authentication scheme created in step 5.

Resources:

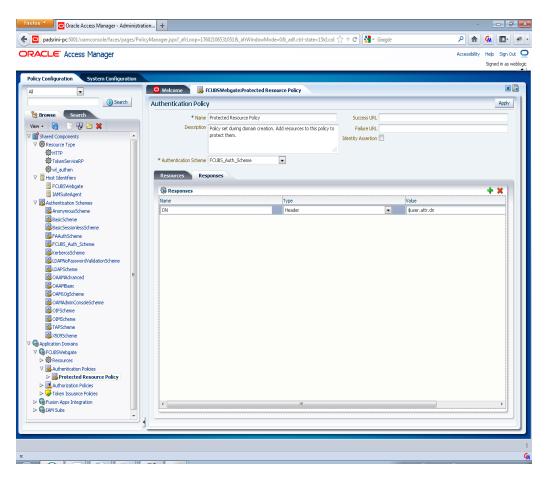
Add the resources which are all need to be protected. If <WebgateName>:/.../ and <WebgateName>:/ are added in the resources then all the sources are protected.





Add DN in the Responses section. Enter the value as *\$user.attr.dn.* The responses maintained in the tab will be added in the response header during the authentication.



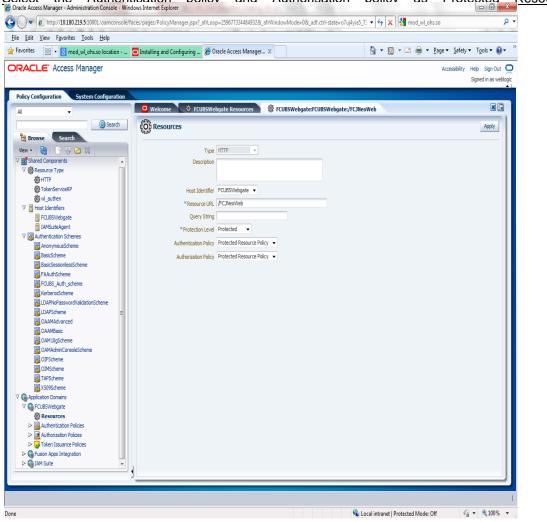


9. Adding Resources

Navigate to Policy Configuration >>Application Domains >>OBTRWebgate >>Resources .

- Click on Create New Resource button .
- Select the type as HTTP.
- Select the Host Identifier as OBTRWebgate
- Enter the resource URL as /FCJNeoWeb
- Select the protection level as Protected
- Click on apply button to update the resource added.





Select the Authentication policy and Authorisation policy as Protected Resource Policy.

10. Adding Authorization Policy

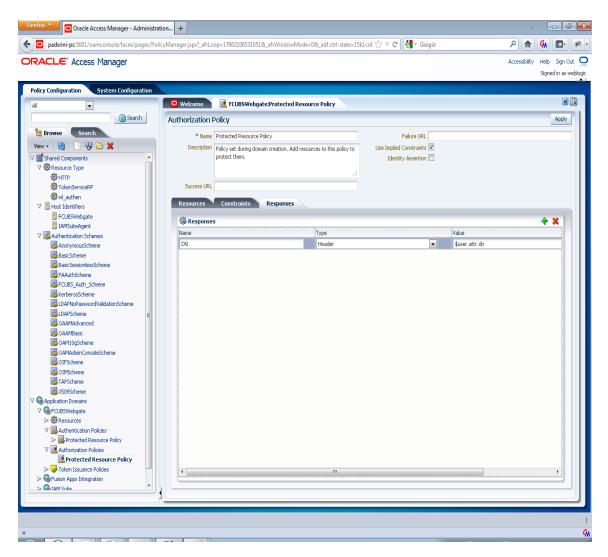
Check whether the resources available in the authentication policies are available in Authorization Policy. During web gate creation these values are defaulted.



| Firefox To 16.14 Setting U | Jp LDAP Synchronization | × ORACLE Identity N | lanager Delegated | × OTN Discussion For | rums : LDAP Sync $	imes$ | Oracle Access Manager - Administrat | × + * | | 0 | X |
|--|---------------------------|------------------------------------|---------------------|---------------------------------|--------------------------|-------------------------------------|--------------|--------|------------|----------|
| e padsrini-pc:7002/oamcor | nsole/faces/pages/PolicyN | /lanager.jspx?_afrLoop=28 | 8567306240326&_afrV | /indowMode=08(_adf.ctrl-s | state=5dqaxo ☆ ⊽ C | 🚼 - 1158/em | P ^ | Cm | D - | * |
| ORACLE Access Ma | nager | | | | | | Accessibilit | y Help | Sign Ou | ut O |
| | - | | | | | | | Signe | d in as w | veblogic |
| Policy Configuration Syst | tem Configuration | | | | | | | | | |
| Al | | 🖸 Welcome 🛛 🛃 | FCUBSWebgate:FCUI | 35_Auth_Policy | FCUBSWebgate:Prote | cted Resource Policy | | | × | |
| | Search | Authorization Policy | | | | | | | Apply | |
| Browse Search | | * Name Protec | ted Resource Policy | | | Failure URL | | | | |
| View 👻 📓 📑 😲 🗁 🗆 | × | | | ion. Add resources to this poli | icy to Use Implie | d Constraints 💟 | | | | |
| ♥ I Shared Components ♥ I Resource Type | <u>^</u> | protec | t them. | | Ider | tity Assertion 📃 | | | | |
| W ser Resource Type | | | | | | | | | | |
| TokenServiceRP | | Success URL | | | | | | | | |
| Ø wl_authen ▽ 📙 Host Identifiers | | Resources Con | nstraints Resp | onses | | | | | | |
| FCUBSWebgate | | | | | | | | | _ | |
| IAMSuiteAgent | | Resources | | | | | | ÷ | <u>×</u> | |
| Authentication Schemes | | Resource URL FCUBSWebgate:/FCJM | leeWeb | | | | • | _ | | |
| BasicScheme | | FCUBSWebgate:/ | leoweb | | | | • | | | |
| BasicSessionlessSchem | ne 👘 | FCUBSWebgate:///* | | | | | • | | | |
| B FAAuthScheme | | 1 CODSWEDGBLEIJIIIJ | | | | | • | | | |
| FCUBS_Auth_Scheme | | | | | | | | | | |
| LDAPNoPasswordValida | ationScheme | | | | | | | | | |
| LDAPScheme | | | | | | | | | | |
| CAAMAdvanced | E | | | | | | | | | |
| CAAMBasic | | | | | | | | | | |
| OAM10gScheme | | | | | | | | | | |
| OAMAdminConsoleScho | eme | | | | | | | | | |
| OIMScheme | | | | | | | | | | |
| TAPScheme | | | | | | | | | | |
| 🔀 X509Scheme | | | | | | | | | | |
| V C Application Domains | | | | | | | | | | |
| ∇ Ger FCUBSWebgate ▷ Or Provide A State | | | | | | | | | | |
| ✓ Specesources ✓ Authentication Policies | | | | | | | | | | |
| FCUBS_Auth_Policy | | | | | | | | | | |
| Protected Resource | e Policy | | | | | | | | | |
| | | | | | | | | | | |
| Protected Resource Vertex Policies | | | | | | | | | | |
| Fusion Apps Integration | ° | | | | | | | | | |
| ▷ C IAM Suite | · · | | | | | | | | | |
| | | | | | | | _ | _ | _ | |
| | | | | | | | | | | _ |
| | | | | | | | | | | 1 |

Add DN in the Responses section. Enter the value as *\$user.attr.dn*. The responses maintained in the tab will be added in the response header during the authorization.





11. Configuring mod_wl_ohs for Oracle Weblogic server Clusters

To enable the Oracle HTTP Server instances to route to applications deployed on the Oracle Weblogic Server Clusters, add the directive shown below to the mod_wl_ohs.sh file available in <Weblogic Home> /Oracle_WT1/instances/instance1/config/OHS/ohs1.

<Location /console>

SetHandler weblogic-handler

WebLogicHost idmhost1.mycompany.com



WeblogicPort 7001

</Location>

12. Checking the Webgate 12c Agent Creation

After configuration of webgate 12c agent launch the URL <u>http://<hostname>:<ohs_Port>/ohs/modules/webgate.cgi?progid=1</u> to verify whether the webgate configuration is fine. If the URL launches a screen as below then the webgate configuration is working fine.



| Access Server | | ection ate | Create | d | tion Num Of Dir ory Threads Infor | ectory mation |
|---|--------|---------------|--|----------------------|--------------------------------------|-------------------------------|
| padsrini-pc 5575, 1 | | 1 | Monday August 27, 201 11:08:0 | y, 2 | | |
| Cache Name | State | | Curr Elems | Timeout (seconds) | | Memory Footprin (bytes) |
| Resource to Authentication Scheme | | 100000 | 60 | 1800 | 13979:416:139:1 | 33688 |
| Authentication Scheme | active | 25 | 1 | 1800 | 45629:140:138:1 | 710 |
| Resource to Authorization Policy | active | 100000 | 59 | 1800 | 183:59:0:1 | 25488 |
| Authorization Result | active | 1000 | 3 | 15 | 178:5:4:1 | 6507 |

13. Using OAM Test Tool (This step is not mandatory)

There is a test tool provided in OAM software which helps us to check the response parameter values. The test tool is available in <OAM Install Dir>\ oam\server\tester.

For eg. D:\weblogic\Middleware\Oracle_IDM1\oam\server\tester



Use *java -jar oamtest.jar* to launch the OAM test tool.

| Oracle Access Manager Test Tool | | | |
|---|-----------------------------|---------------------------|-----------------|
| <u>File E</u> dit <u>T</u> est <u>H</u> elp | | | |
| 🖻 🖥 🥔 🔁 | | | |
| Server Connection | | | |
| Primary: padsrini-pc | | *Agent ID FCUBSWebgate | |
| Primary. padsimi-pc [35. | 1 | Agent Password | |
| Secondary: 0 | 1 | | ? |
| Min Conn Timeout (ms) Mode 1 30000 open v | | × | Connect |
| Protected Resource URI | | | * |
| Scheme *Host | | Port | ▼ € |
| http FCUBSWebgate | | 0 | Get Auth Scheme |
| Resource /FCJNeoWeb | | Operation Get 🗸 🔗 | Validate |
| | | | |
| User Identity | | | |
| IP Address *Username | Password | | <i>🖉</i> |
| SARAN | •••••• | • ? 🗸 | Authenticate |
| User Certificate Store | | v | Authorize |
| | | | |
| Status Messages | | | |
| [8/27/12 11:17 AM][response] Redirect URL : https://pa [8/27/12 11:17 AM][response] Credentials expected : 0 | | | * |
| [8/27/12 11:17 AM][request][authenticate] yes | | | |
| [8/27/12 11:17 AM][response] User DN : on=SARAN,or [8/27/12 11:17 AM][response] SessionID : 965398ea-7 | | | |
| [8/27/12 11:17 AM][response][action] DN : cn=SARAN | l,cn=users,dc=oracle,dc=com | | |
| [8/27/12 11:17 AM][response][action] OAM_IMPERSO [8/27/12 11:17 AM][request][authorize] yes | DNATOR_USER : | | = |
| [8/27/12 11:17 AM][response][action] DN : cn=SARAN | | | |
| [8/27/12 11:17 AM][response][action] OAM_IMPERSO [8/27/12 11:17 AM][response][action] OAM_REMOTE | | | |
| [8/27/12 11:17 AM][response][action] OAM_IDENTITY | - | e | |
| | | | |
| Elapsed (ms): 47 Capture Queue: E | mpty | | 6 🥔 |



3.4 First launch of ORACLE BANKING TREASURY MANAGEMENT after Installation

After installing ORACLE BANKING TREASURY MANAGEMENT and while launching it for first time, the normal OBTR login screen with userid and password will appear, this is because when installing the 'sso installed' parameter will be set to 'N'.

3.4.1 SSO Parameters

After enabling SSO, the parameters required for SSO should be maintained. Go to "Security Maintenance -> Sys. Administration -> SSO Maintenance". Provide all the details like Directory Server host name, Port number, LDAP admin Userid , admin Password, LDAP base and Login time out duration (in Sec).

| - | Single Sign On Maintenance | | | | | | | - | × |
|---|--|---|---|--------|---|---|---|-------|---|
| | Save | | | | | | | | |
| | LDAP Host * LDAP Port * LDAP Admin Id * LDAP Password * | CUSer_A Cuser | 0 | | | | | | |
| | Maker Checker | Date Time: Date Time: | | Mod No | 2 | Record Status Open Authorization Status | с | ancel | |

3.4.2 Maintaining LDAP DN for OBTR Users

For each user id in OBTR a user has to be created in the LDAP.



When creating the user in LDAP ensure that the DN used is same as the LDAP DN value that will be updated in user maintenance form. Once the user is created in LDAP go to the user creation form in OBTR. If the OBTR user already exists then unlock the user and update the LDAP DN value which was set when creating the user in LDAP. Click on Validate button to check whether any other user is having the same LDAP DN value.

| Jser Creation | | | | |
|-------------------------------|------------|--------------------------|----------------------|--|
| Save | | | | |
| User Details | | User Password | | |
| User Identification * OBTFUSE | ĒR | Password | ••••• | |
| Name * OBTF Use | er | Password Changed On | | |
| LDAP DN OBTFUSE | ER 🔎 | Email | | |
| Validate | | Status Changed On | | |
| MFA ID | | Reference Number | | |
| MFA Enabled Disabled | T | User Status | | |
| Home Entity * ENTITY_ | | | O Hold O Disabled | |
| | | | O Locked | |
| Date | | | | |
| Start Date * 2020-03-1 | | | | |
| End Date YYYY-MM | I-DD | | | |
| Invalid Logins | | Screen Saver Details | | |
| No of Cumulativo Logino | 0 | Saraanaayar Intarial /in | | |
| Restricted Password | | | | |
| Maker | Date Time: | Mod No | Record Status | |
| Checker | Date Time: | | Authorization | |

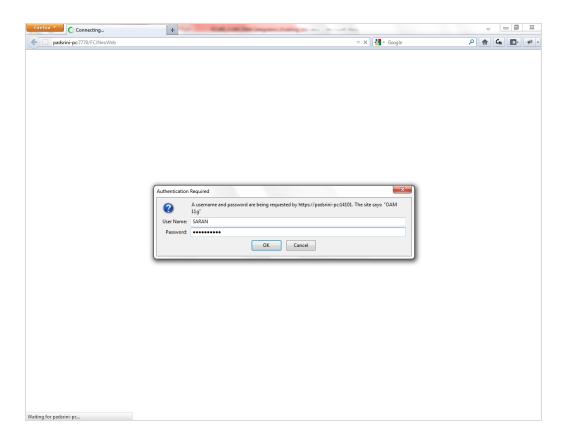
3.4.3 Launching ORACLE BANKING TREASURY MANAGEMENT

After setting up ORACLE BANKING TREASURY MANAGEMENT to work on Single Sign on mode, navigate to the interim servlet URL from your browser.

For e.g.: http://<hostname>:[port]/FCJNeoWeb

Since the resource is protected, the WebGate challenges the user for credentials as shown below.





Once the user is authenticated and authorized to access the resource, the servlet gets redirected to normal ORACLE BANKING TREASURY MANAGEMENT application server URL and now the new signon form will appear as below. The application will automatically redirect ORACLE BANKING TREASURY MANAGEMENT home page.



| S Oracle Financial Services - Google Chrome | | | _ | |
|---|---|------------------------|---------------|-------|
| Not secure whf00fqn:7058/FCJNeoWeb/LoginServlet | | | | |
| ORACLE | Font Size: A A A | Theme: Cadet Green | Glaucous Dark | Sepia |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Oracle FLEXCUBE Trade Finance | | | |
| | User ID | | | |
| | | | | |
| | | | | |
| | Password | | | |
| | Cian In | | | |
| | Sign In | | | |
| | | | | |
| | Copyright © 2017,2018, Oracle and/or its affiliates | . All rights reserved. | | |

3.4.4 Signoff in a SSO Situation

ORACLE BANKING TREASURY MANAGEMENT does not provide for single signoff currently, i.e., when a user signs off in ORACLE BANKING TREASURY MANAGEMENT, the session established with Oracle Access Manager by the user will not be modified in any manner.

In a SSO situation the 'Exit' and 'Logoff' actions in ORACLE BANKING TREASURY MANAGEMENT will function as 'Exit', i.e., on clicking these, the user will 'exit' ORACLE BANKING TREASURY MANAGEMENT and will need to re-launch ORACLE BANKING TREASURY MANAGEMENT using the ORACLE BANKING TREASURY MANAGEMENT launch URL.





Oracle Access Manager

[April] [2020]

Version 14.4.0.0.0

Oracle Financial Services Software Limited Oracle Park Off Western Express Highway Goregaon (East) Mumbai, Maharashtra 400 063 India Worldwide Inquiries: Phone: +91 22 6718 3000 Fax: +91 22 6718 3001 https://www.oracle.com/industries/financial-services/index.html

Copyright © [2020], Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.